



PC/2098/00181

RECD 16 SEP 1998

WIPO

PCT

EJK

РОССИЙСКОЕ АГЕНТСТВО ПО ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ
(РОСПАТЕНТ)

ФЕДЕРАЛЬНЫЙ ИНСТИТУТ ПРОМЫШЛЕННОЙ СОБСТВЕННОСТИ

09/622047

рег.No 20/14-347

11 августа 1998 года

СПРАВКА

Федеральный институт промышленной собственности Российского Агентства по патентам и товарным знакам настоящим удостоверяет, что приложенные материалы являются точным воспроизведением первоначального описания, формулы и чертежей (если имеются) заявки на выдачу патента на изобретение N 98103646, поданной в феврале месяце 24 дня 1998 года.

Название изобретения: Способ блочного шифрования дискретных данных.

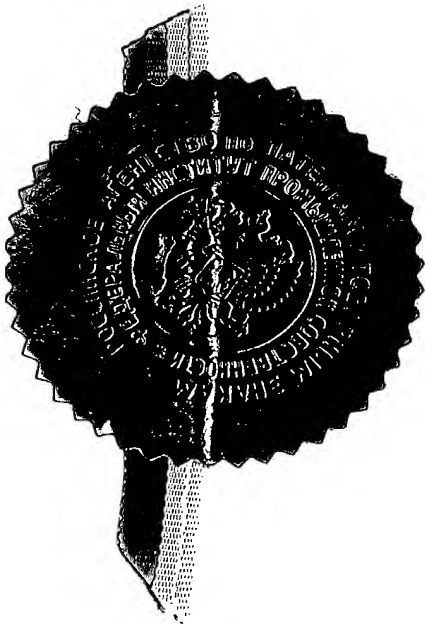
Заявитель (и): МОЛДОВЯН Александр Андреевич.

Действительные авторы: МАСЛОВСКИЙ Владимир Михайлович,
МОЛДОВЯН Александр Андреевич,
МОЛДОВЯН Николай Андреевич.

PRIORITY DOCUMENT

Уполномоченный заверить копию
заявки на изобретение

Г.Ф.Востриков
Заведующий отделом



98103646

Экз. N

МПК⁶ H 04 L 9/00

СПОСОБ БЛОЧНОГО ШИФРОВАНИЯ ДИСКРЕТНЫХ ДАННЫХ

Изобретение относится к области электросвязи и вычислительной техники, а конкретнее к области криптографических способов и устройств для шифрования сообщений (информации). В совокупности признаков заявляемого способа используются следующие термины:

-секретный ключ представляет из себя комбинацию битов, известную только законному пользователю;

-ключ шифрования представляет из себя комбинацию битов, используемую при шифровании информационных сигналов данных; ключ шифрования является сменным элементом шифра и используется для преобразования данного сообщения или данной совокупности сообщений; ключ шифрования формируется по детерминированным процедурам по секретному ключу; в ряде шифров в качестве ключа шифрования используется непосредственно секретный ключ;

-шифр представляет собой совокупность элементарных шагов преобразования входных данных с использованием шифрключа; шифр может быть реализован в виде программы для ЭВМ или в виде отдельного электронного устройства;

-подключ представляет собой часть ключа шифрования, используемую на отдельных элементарных шагах шифрования;

-шифрование есть процесс, реализующий некоторый способ преобразования данных с использованием шифрключа, переводящий данные в криптограмму, представляющую собой псевдослучайную последовательность знаков, из которой получение информации без знания ключа шифрования практически невыполнимо;

-дешифрование есть процесс, обратный процедуре шифрования; дешифрование обеспечивает восстановление информации по криптограмме при знании ключа шифрования;

-криптостойкость является мерой надежности защиты информации и представляет собой трудоемкость, измеренную в количестве элементарных операций, которые необходимо выполнить для восстановления информации по криптограмме при знании алгоритма преобразования, но без знания ключа шифрования.

Известны способы блочного шифрования данных, см. например стандарт США DES [У.Диффи, М.Э.Хеллмэн. Защищенность и имитостойкость: Введение в криптографию// ТИИЭР. 1979. Т. 67. N. 3. С. 87-89], способ шифрования по патенту США N 5222139, от 22 июня 1993 г., шифр FEAL-1 и криптоалгоритм В-Crypt [С.Мафтик. Механизмы защиты в сетях ЭВМ.- М., Мир, 1993. С. 49-52]. В известных способах шифрование блоков данных выполняют путем формирования ключа шифрования в виде совокупности подключей, разбиения преобразуемого блока данных на подблоки и поочередного изменения последних с помощью операций подстановки, перестановки и арифметических операций, выполняемых над текущим подблоком и текущим подключом.

Однако, известные способы-аналоги не обладают достаточной стойкостью к дифференциальному криптоанализу [Berson T.A. Differential Cryptanalysis Mod 2^{32} with application to MD5// EUROCRYPT'92. Hungary, May 24-28, 1992. Proceedings. P. 67-68], т.к. для всех входных блоков данных для заданного шага преобразования используется один и тот же подключ в неизменном виде.

Наиболее близким по своей технической сущности к заявляемому способу блочного шифрования является способ, описанный в Российском стандарте криптографической защиты данных [Стандарт СССР ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования]. Способ прототип включает в себя формирование ключа шифрования в виде последовательности из 8 подключей длиной 32 бита, разбиении входного 64-битового блока данных на два 32-битовых подблока B_1 и B_2 и поочередном преобразовании подблоков. Один шаг преобразования подблока, например подблока B_2 , заключается в наложении на него текущего подключа Q_i , являющегося фиксированным для данного шага, с помощью операции сложения по модулю 2^{32} (\boxplus) в соответствии с формулой $B_2 := B_2 \boxplus Q_i$, где $1 \leq i \leq 8$, после чего над полученным новым значением подблока B_2 выполняют операцию подстановки, затем операцию циклического сдвига влево на одиннадцать бит, т.е. на одиннадцать двоичных разрядов в сторону старших разрядов, а затем на полученное значение B_2 накладывают подблок B_1 с помощью операции поразрядного суммирования по модулю два (\oplus) в соответствии с формулой $B_2 := B_2 \oplus B_1$. Операция подстановки выполняется следующим образом. Подблок разбивается на 8 двоичных вектора длиной по 4 бит. Каждый двоичный вектор заменяется двоичным вектором из таблицы подстановок. Выбранные из таблицы подстановок 8 4-битовых вектора объединяются в 32-битовый двоичный вектор,

который и является выходным состоянием подблока после выполнения операции подстановки. Всего выполняется 32 аналогичных шага изменения подблоков, причем для всех преобразуемых входных блоков данных на фиксированном шаге преобразования подблоков используется один и тот же подключ с неизменным значением.

Однако, способ прототип имеет недостатки, а именно, микроэлектронные устройства шифрования на его основе являются дорогостоящими и не обеспечивают высокой скорости шифрования [Андреев Н.Н. О некоторых направлениях исследований в области защиты информации//Сборник материалов международной конференции 'Безопасность информации'. Москва, 14-18 апреля 1997. М. 1997. С. 96], необходимой для построения средств защиты информации, работающих в масштабе реального времени. На основе способа прототипа очень сложно создать на современной элементной базе устройства, обеспечивающие скорость шифрования более 10 Мбит/с. Этот недостаток связан с тем, что для обеспечения стойкости к дифференциальному криптоанализу в способе прототипе используется большое число операций четырех типов, включая операции подстановки.

В основу изобретения положена задача разработать способ шифрования, в котором преобразование входных данных осуществлялось бы таким образом, чтобы обеспечивалось уменьшение числа операций преобразования, приходящихся на один бит входных данных, при одновременном обеспечении высокой стойкости к дифференциальному криптоанализу, благодаря чему повышается скорость шифрования.

Поставленная задача достигается тем, что в способе блочного шифрования дискретных данных, включающем формирование ключа шифрования в виде совокупности подключей, разбиение блока данных на $N \geq 2$ подблоков и поочередное преобразование подблоков путем выполнения двухместной операции над подблоком и подключом новым согласно изобретению является то, что перед выполнением двухместной операции над i -тым подблоком и подключом над подключом выполняют операцию перестановки, зависящую от j -того подблока, где $j \neq i$.

Благодаря такому решению структура подключей, используемых на заданном шаге шифрования, зависит от преобразуемых данных и тем самым на данном шаге преобразования для различных входных блоков используются различные модифицированные значения подключей, благодаря чему обеспечивается высокая стойкость к дифференциальному криптоанализу при одновременном уменьшении числа выполняемых операций преобразования, что и обеспечивает повышение скорости криптографического преобразования.

Ниже сущность заявляемого изобретения более подробно разъясняется примерами его осуществления со ссылками на прилагаемые чертежи.

На фиг. 1 представлена обобщенная схема шифрования согласно заявляемому способу.

На фиг. 2 схематично представлена структура блока управляемых перестановок, состоящего из совокупности однотипных элементарных блоков, реализующих перестановку двух соседних двоичных разрядов (битов) в зависимости от управляющего сигнала u .

На фиг. 3 представлена блок-схема элементарного управляемого переключателя, являющегося базовым элементом блока управляемых перестановок. При $u = 1$ входные биты не переставляются, т.е. сигналы на выходе совпадают с сигналами на входе. При $u = 0$ входные биты переставляются.

На фиг. 4 представлена таблица входных и выходных сигналов элементарного управляемого переключателя при высоком потенциале управляющего сигнала.

На фиг. 5 представлена таблица входных и выходных сигналов элементарного управляемого переключателя при низком потенциале управляющего сигнала.

Изобретение поясняется обобщенной схемой криптографического преобразования блоков данных на основе заявляемого способа, которая представлена фиг. 1, где: P — блок управляемых перестановок; A и B — преобразуемые n -битовые подблоки; K_{2r} , K_{2r-1} — элементы ключа шифрования (подключи); знак \oplus обозначает операцию поразрядного суммирования по модулю два, знак \boxplus — операцию суммирования по модулю 2^n . Жирные сплошные линии обозначают шину передачи n -битовых сигналов, тонкие пунктирные линии — передачу одного управляющего бита. Жирные пунктирные линии — шину передачи n управляющих сигналов, в качестве которых используются биты преобразуемых подблоков.

Фиг. 1 показывает один (r -тый) раунд шифрования. В зависимости от конкретной реализации блока управляемых перестановок и требуемой скорости преобразований могут быть заданы от 6 до 20 и более раундов.

Рассмотрим конкретные примеры реализации заявляемого способа криптографических преобразований блоков двоичных данных.

Пример 1.

В данном примере поясняется шифрование 64-битовых блоков данных. Ключ шифрования формируется в виде 16 подключей $K_1, K_2, K_3, \dots, K_{16}$, каждый из которых имеет длину 32 бит. Входной блок данных разбивается на два 32-битовых подблока A и B . Шифрование входного блока

описывается следующим алгоритмом:

1. Установить счетчик числа раундов $r = 1$.
2. Преобразовать подблок B в соответствии с выражением:

$$B := B \oplus P_A(K_{2r}),$$

где $P_A(K_{2r})$ обозначает операцию перестановки битов подключа K_{2r} , выполняемую в зависимости от значения подблока A .

3. Преобразовать подблок A в соответствии с выражением:

$$A := A + B.$$

4. Преобразовать подблок A в соответствии с выражением:

$$A := A \oplus P_B(K_{2r-1}),$$

где $P_B(K_{2r-1})$ обозначает операцию перестановки битов подключа K_{2r-1} , выполняемую в зависимости от значения подблока B .

5. Преобразовать подблок B в соответствии с выражением:

$$B := B + A.$$

6. Если $r \neq 8$, то прирастить счетчик $r := r + 1$ и перейти к шагу 2, в противном случае СТОП.

На фиг. 2, где тонкие сплошные линии обозначают передачу одного бита подключа, показана возможная реализация блока управляемых перестановок, использующая совокупность элементарных переключателей S . Данный пример блока управляемых перестановок соответствует блоку 8P с 8-битовым входом для сигналов подключа и 8-битовым входом для управляющих сигналов (битов подблока данных), обозначенных пунктирными линиями аналогично обозначению на фиг. 1. Структура блока ^{32}P управляемых перестановок с 32-битовым входом для сигналов подключа и 32-битовым входом для управляющих сигналов подблока данных является аналогичной блоку 8P , представленному на фиг. 2. Такая структура управляемого блока перестановок задает число различных вариантов операции перестановки равное числу возможных кодовых комбинаций на входе управления. Для ^{32}P число различных перестановок равно 2^{32} . Это означает, что при шифровании двух различных блоков данных вероятность повторения некоторой перестановки на заданном шаге равна 2^{-32} , а повторение перестановок на z заданных шагах равна 2^{-32z} . Таким образом, набор модифицированных подключей, используемых для преобразования каждого входного сообщения, является уникальным. Фиг.

3, 4 и 5 поясняют работу элементарного переключателя, где u — управляющий сигнал, a и b — линии передачи однобитовых входных сигналов, c и d — линии выходных сигналов. Таблицы на фиг. 4 и 5 показывают зависимость выходных сигналов от входных и управляющих сигналов. Из данных таблиц видно, что при $u = 1$ линия a коммутируется с линией c , а линия b — с линией d . При $u = 0$ линия a коммутируется с линией d , а линия b — с линией c . Для современной планарной технологии изготовления интегральных схем описанная структура блоков управляемых перестановок является простой, благодаря чему легко осуществить изготовление криптографических микропроцессоров, содержащих управляемые блоки перестановок с размером входа 32, 64 и 128 бит.

Приведенные примеры показывают, что предлагаемый способ блочного шифрования дискретных данных технически реализуем и позволяет решить поставленную задачу.

Заявляемый способ может быть реализован, например, в специализированных криптографических микропроцессорах, обеспечивающих скорость шифрования порядка 300 Мбит/с, достаточную для шифрования в масштабе реального времени данных, передаваемых по скоростным оптоволоконным каналам связи.

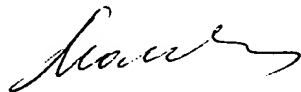
Авторы:



Масловский В.М.



Молдовян А.А.



Молдовян Н.А.

ФОРМУЛА ИЗОБРЕТЕНИЯ

Способ блочного шифрования дискретных данных, включающий формирование ключа шифрования в виде совокупности подключей, разбиение блока данных на $N \geq 2$ подблоков и поочередное преобразование подблоков путем выполнения двухместной операции над подблоком и подключом, отличающийся тем, что перед выполнением двухместной операции над i -тым подблоком и подключом над подключом выполняют операцию перестановки, зависящую от j -того подблока, где $j \neq i$.

Авторы:



Масловский В.М.

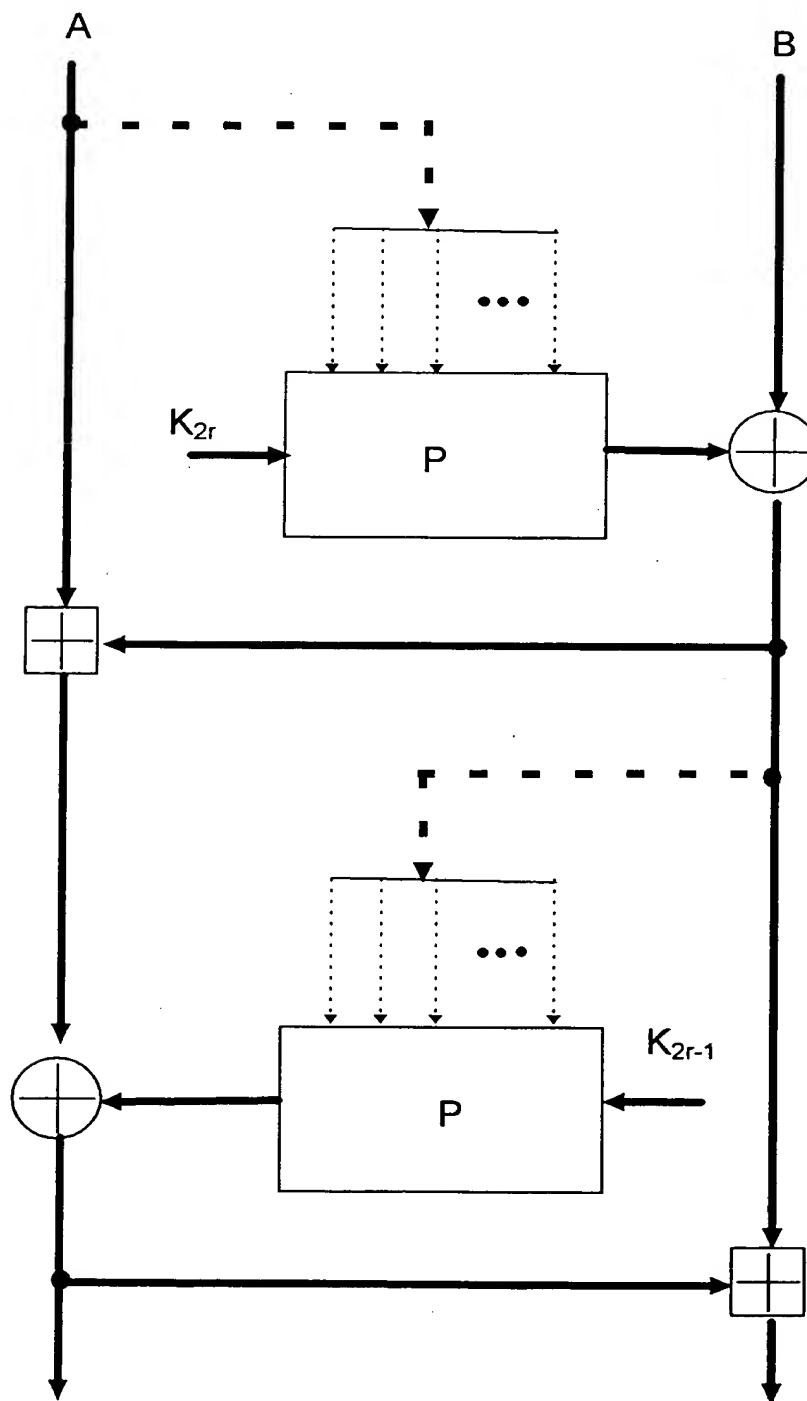


Молдовян А.А.



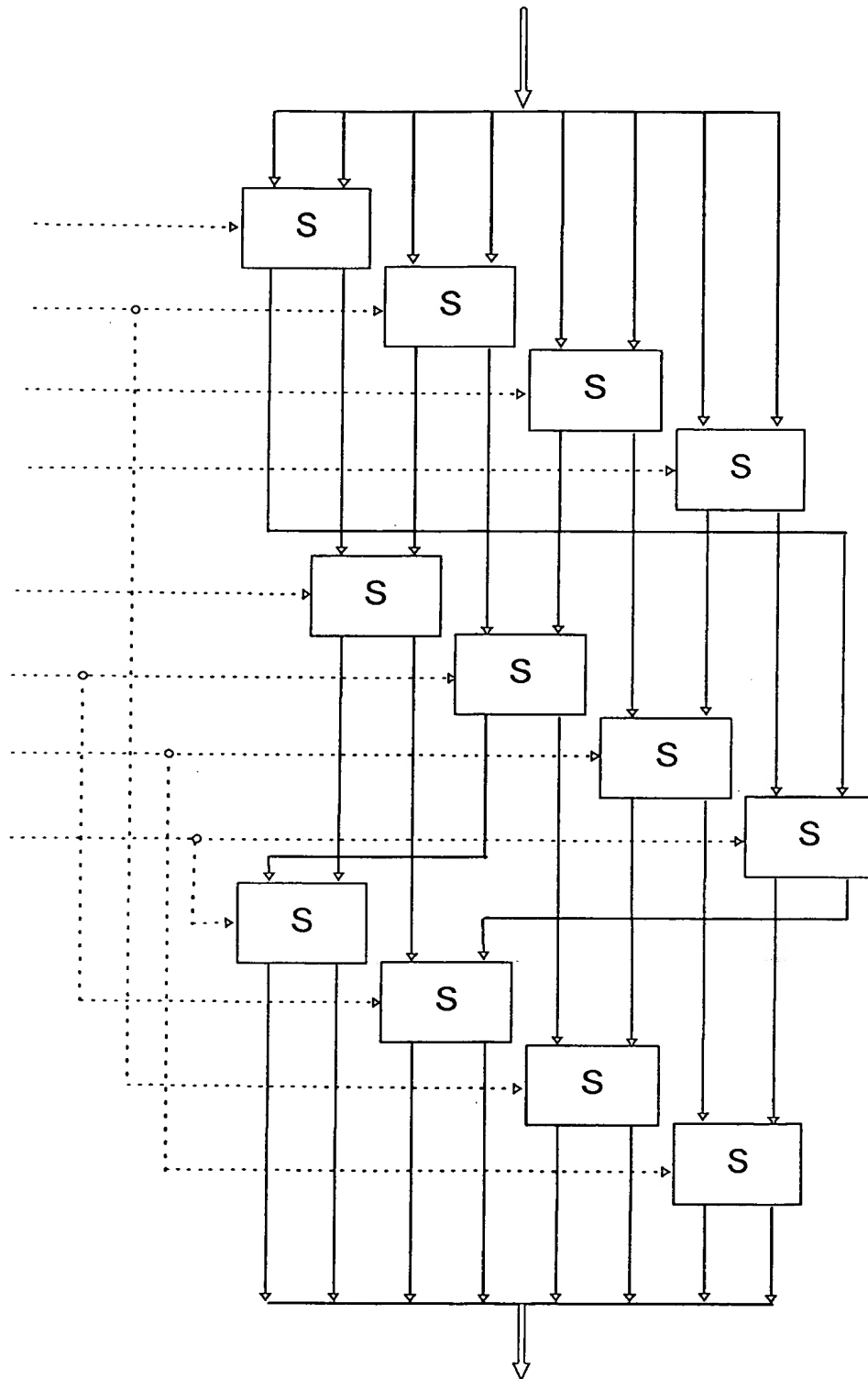
Молдовян Н.А.

СПОСОБ БЛОЧНОГО ШИФРОВАНИЯ ДИСКРЕТНЫХ ДАННЫХ



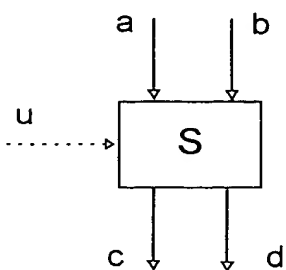
Фиг.1.

СПОСОБ БЛОЧНОГО ШИФРОВАНИЯ ДИСКРЕТНЫХ ДАННЫХ



Фиг.2.

СПОСОБ БЛОЧНОГО ШИФРОВАНИЯ ДИСКРЕТНЫХ ДАННЫХ



Фиг.3.

u=1

ВХОД		ВЫХОД	
a	b	c	d
1	0	1	0
0	1	0	1
0	0	0	0
1	1	1	1

Фиг.4.

u=0

ВХОД		ВЫХОД	
a	b	c	d
0	1	1	0
1	0	0	1
0	0	0	0
1	1	1	1

Фиг.5.

Экз. N

РЕФЕРАТ

СПОСОБ БЛОЧНОГО ШИФРОВАНИЯ
ДИСКРЕТНЫХ ДАННЫХ

Изобретение относится к области электросвязи и вычислительной техники, а конкретнее к области криптографических способов и устройств для шифрования данных. Целью изобретения является повышения скорости шифрования. Способ включает формирование ключа шифрования в виде совокупности подключей, разбиение блока данных на $N \geq 2$ подблоков и поочередное преобразование подблоков путем выполнения двухместной операции над подблоком и подключом. Отличается от известных способов тем, что перед выполнением двухместной операции над i -тым подблоком и подключом над подключом выполняют операцию перестановки, зависящую от j -того подблока, где $j \neq i$.

Ф.и.-1, Илл.- 5.